CYRIS360

Organizational security

October 2024 – Version 1.2
Classification: Public

Unleashing Cyber Resilience in Every Direction.

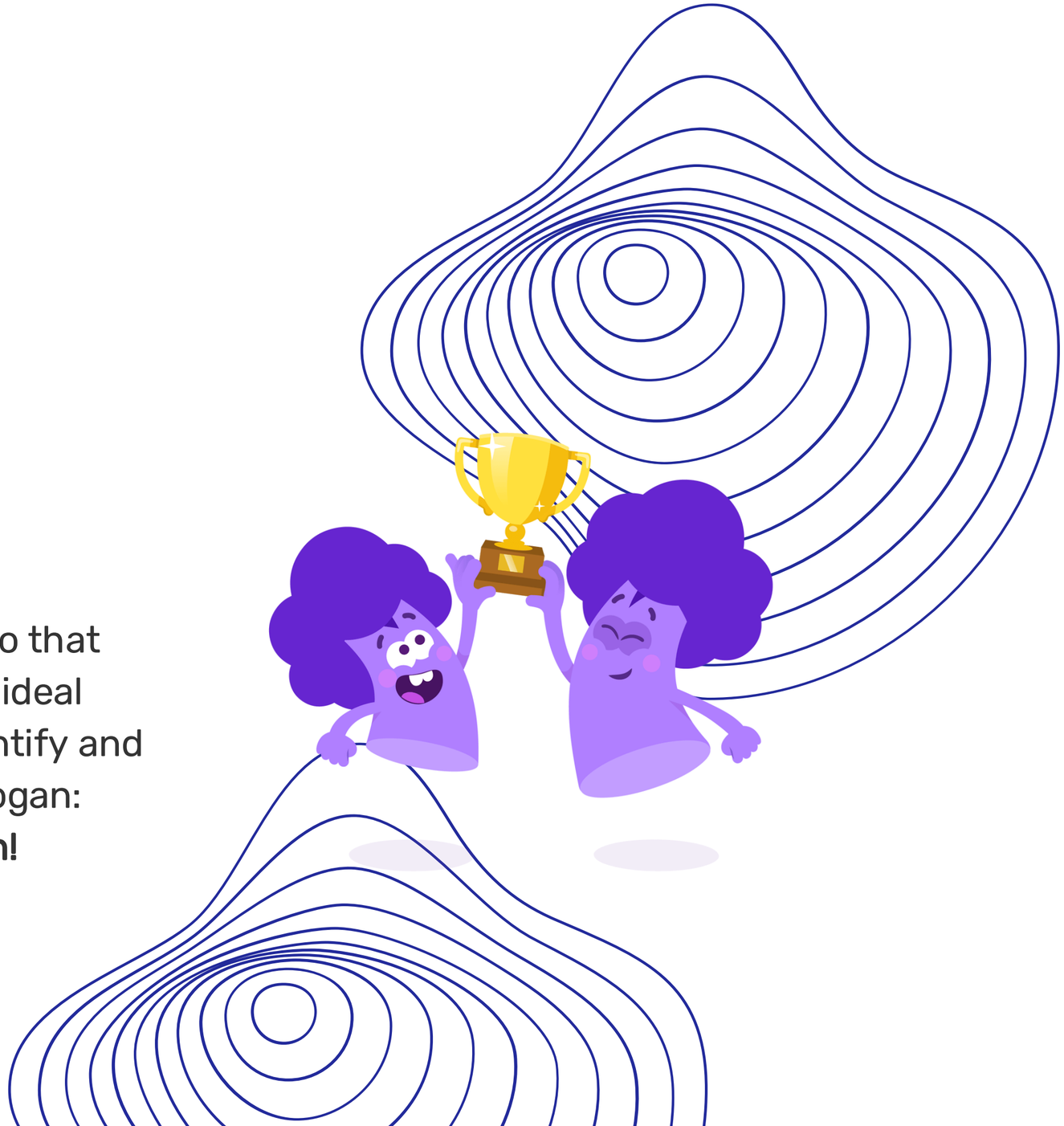
Organizational Service portfolio

Overview

Our value proposition

Transform cyber risks from business inhibitor to a business enabler.

Clients are always in control of all cyber risks.
Our value proposition is to facilitate this task so that you can invest all your energy on creating the ideal product and/or service, while we help you identify and mitigate all potential cyber risks. Hence our slogan:
Unleashing Cyber Resilience in Every Direction!



CYRIS360

1. Organizational assessment/audit

Final report delivered within 5 business days.

Fixed & Transparent price:

- 2900 euros for small and medium organizations (up to 250 FTE).
- 1900 euros for micro-organization (up to 50 FTE).

Gap assessment

Evaluate the current maturity level and identify potential gaps and area for improvements

Physical security assessment

Check the security controls on premises, such as physical access control and physical network security.

Internal audit

Review an existing management system and evaluate the effectiveness of implemented controls

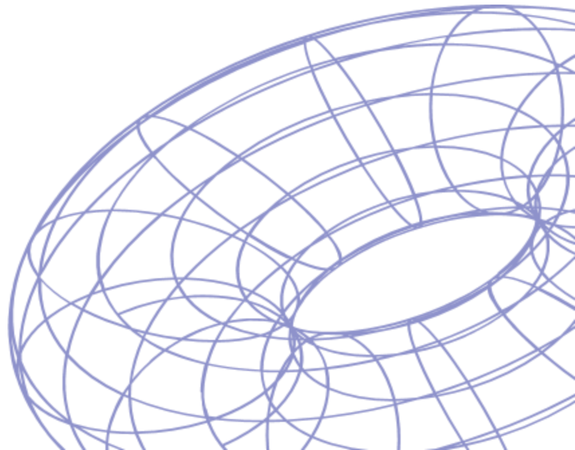
Note: All prices are excluding VAT.

2. Implementation of management systems

Reduce the risks related to information security

Earn customer's trust

Increase your competitive advantage



The ISO High Level Structure

(aka: Annex L)

Step 1

Plan

4-Context of the organization
5-Leadership
6-Planning

Step 2

Do

7-Support
8-Operation

Step 3

Check

9-Performance Evaluation

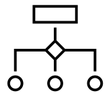
Step 4

Act

10-Improvement

2.1 ISO/IEC 27001

Implement information security requirements (ISO Annex L) with 93 controls grouped in 4 categories

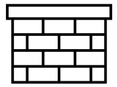


Organizational

37 controls related to the ISMS documentation such as general policies and processes.

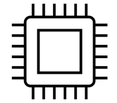
People

8 controls related to managing your staff such as onboarding and offboarding processes.



Physical

14 controls related to the organization's premises such as employee access to secure areas.



Technological

34 controls related to systems, cryptography, software and network to protect the assets.

2.2 ISO 22301

Relevant if Business Continuity is important for you/your customers. Also uses ISO Annex L structure.

Certifiable standard – can be implemented independently or in combination with ISO27001

Examples:

- Energy & Utilities
- Telecom service providers
- Mobility solutions providers
- Banking, Payment and FinTech

2.3 TISAX ISA

Relevant for Automotive industry in EU

Extends ISO27001 with topic-specific guidance, and include 6 maturity levels:

- Incomplete
- Performed
- Managed
- Established
- Predictable
- Optimized

Examples:

- Automotive OEMs
- Automotive suppliers

2.4 NEN 7510

Healthcare data protection (NL only)

Certifiable standard – extends ISO27001 with 35 additional controls.

Examples:

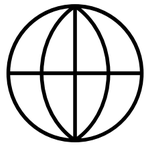
- Hospitals
- Clinics
- Pharmacies

3. Information security trainings & workshops

-

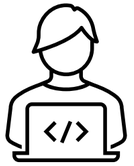
Basic information security awareness

2-4 hours group workshop for general information security awareness topics



ISO/IEC 27001 implementer

Specialized training for personnel involved in ISMS implementation.
4 days course excluding the exam (Receive a Certificate from PECB)



Secure Software Lifecycle

Specialized course for Software developers and lead architect.
Topics: Secure coding & Threat modeling / TARA

4. Additional organizational services

We can help you build and strengthen your in-house capability with our specialized and tailored organizational services

Infrastructure

We help our clients protect their digital infrastructure (On-prem & Cloud) by reducing the attack surface and implementing secure communication (Including TLS configuration)

IAM

We help our clients implement Identity and access management (IAM) best practices, such as multifactor authentication, least privilege, and separation of duties.

DLP

We help our clients protect their data by implementing Data Loss Prevention (DLP).

SOC

We help our client detect and respond to unusual & suspicious activities by implementing a Security Operation Center (SOC)

5. Relevant EU Regulations

4.1 NIS2

NIS2 regulation apply to entities that operates in certain (critical) sectors, if these are qualified as important or essential entities.

- Information security policy
- Incident handling
- Business continuity
- Supply chain security
- Network security
- Risk management
- Cyber hygiene & Training
- Use of cryptography

4.2 DORA

DORA relates explicitly to EU financial services, focusing on maintaining cybersecurity resilience.

- ICT Risk Management Framework
- Incident Management and Reporting
- Compliance Management and Reporting
- Operational Resilience
- Supply chain security

Do you have any questions?

Let us know: we are happy to help!

info@cyris360.com

www.cyris360.com

CYRIS360